VOLUME 2 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CYBERCRIME INVESTIGATION CHALLENGES

- Divyanshu Devang[1]

ABSTRACT

The swift advancement of computer technology, as well as the convergence of computer and communication technology, has brought about substantial shifts in the information-related activities of humans. Firstly, the computer has emerged as the preeminent instrument for the processing of data as a direct result of the power and efficiency of information processing. As a direct consequence of this, ever more information is being processed and saved in computer systems. Second, the Internet's ability to transcend borders and cultures has helped it become one of the most important channels for human communication. As a consequence of this, our society is undergoing a transition toward a "virtual society," which is a society in which people's day-to-day activities, such as shopping, obtaining services, and especially sharing information, can be accomplished without having direct contact with other people. These days, computers and computer networks can be found almost anywhere and are utilized in every conceivable aspect of contemporary society. In spite of the fact that the proliferation of information technology has made it possible for global businesses to thrive, it has also become one of the most important tools that unscrupulous people use to commit crimes and evade capture by authorities. Investigation and forensics of cybercrime are frequently cited as the most significant obstacle facing law enforcement agencies in the 21st century. This paper will discuss the challenges that are currently being faced by law enforcement agencies and will make an attempt to look into the future in order to identify the research directions that are being pursued in the fields of computer forensics and cybercrime investigation.

[1] LL.M. Candidate at Chanakya National Law University, Patna

INTRODUCTION

Computer technology has both advantages and disadvantages. Regardless of the fact that computers make life easier and faster, they are prone to the most serious form of crime known as cyber-crime. The whole company and government functions would almost cease to exist if not for computer technology. The broad availability of low-cost, high-performance, and user-friendly computers has allowed number of individuals to utilise and, more importantly, rely on computers in their daily lives i.e health sector, railway ticketing, communication, smart cities project etc. As a response, the current work explains a systematic understanding of cyber-crime and its effects on other various fields, including socio-economic, consumer trust and political, as well as future cyber-crime trends. Any criminal behaviour involving in use of computer system or technology is referred to as computer crime. As our lives have become more dependant on current information technology, it is vital to strengthen cyber crime investigative methods, especially when dealing with extremely sensitive information of Government, military secrets, bank data and other personal information. Unapproved access approach to any computer source information with the intention of changing, destroying, or stealing any such digital data or information, as revealed in a cybercrime investigation. Financial losses or the loss of sensitive information, as well as the release or destruction of top-secret, private, or confidential information, may occur from such suspicious behaviour. As a result, by examining latest developments in the nation's Broadband network, also the need for information security laws in the countries, this paper examines the main challenges that the Indian States (Bihar, Uttar Pradesh, Maharashtra, Jharkhand, and Delhi) face in the computer crime investigation system.

On the Internet Credit card information theft has now considered a well-known fraud or threat. So the cybercrime which is reported to the “National Cyber Crime Reporting Portal” are child-abuse/pornography, fraud, and Electronic mail spoofing.

Also we look at the difficulty of identifying and monitoring computer crime as well as the effectiveness of various approaches for preventing or prosecuting such computer crimes.

“Cyber-crime means that computer system uses as a tool to facilitate unlawful purposes or aims like online fraud or theft, child pornography, intellectual property, identity theft, or infringing privacy is known as cyber crime. As the computer system has become essential to trade or commerce, entertainment, and government function, cybercrime has gained signifiance, especially through the Internet.[2] Cybercrime has the ability to disrupt any railway system, send out false signals to misdirect planes on their flight, leak sensitive military data to various countries, block e-media, and drag down any system in a matter of seconds. Since from year 2020, the world has been seized by a tremendous global pandemic (Covid-19) that has profoundly altered the way individuals and entities operate and interact with one another. This global pandemic has also resulted new cyber risks, as well as the growth of old threats from criminal groups and nation- states. This introduction outlines some of the most important cyber threat vectors related to COVID-19 that have arisen in the last year.

The objective of this research is to look at some of the aspects, consequences, and future prospects of cyber-technology, with an emphasis on the cybercrime danger that India faces. Efforts were made to look into India's legal structure to see whether it can be used to control it.

HISTORY OF CYBER CRIME

Cybercrime's history and evolution are easy to understand, as they reflect the evolution of the Internet. Of course, the initial crimes were basic cyberattacks to steal data from local networks, but as the Internet grew rapidly, as such did the attacks. The first cybercrime was recorded, in the year 1820, this is not astonishing which provided under the abacus, and considered as primary form of a computer which has been used in the countries like India, China and Japan since 3500 Common Era The invention of the computer's with "analytical engine of Charles Babbage's" whom we known as Father of Computer. Since then, computers have come a long way, with neural networks and nano-computing promising to tum each and every atom in a glass of water into a computer capable of billions of functions per second. Cybercrime is a contemporary problem that originates from our increasing dependence over technology. Cybercrime has taken place on enormous ratio in a period when the whole thing from fridges and microwave ovens to nuclear power plant is managed with the aid of using computers.[3]

[2] Michael Aaron Dennis, Cyber Crime, 1 Feb 2022, (10:04 A.M), https://www.britannica.com/topic/cybercrime.

[3] Vol. 4 (5),2013, RajarshiRaiChoudhury et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, , 729-732.

CONCEPTUAL STUDY OF 'INFORMATION AND COMMUNICATION TECHNOLOGY'

The "International Telecommunication Union" (ITU) published report on the Concept of Cybercrime phenomena, challenges and legal response with the objective of helping countries in better understanding the legislative aspects of cyber security and harmonising legal frameworks. The purpose of report to assist the developed or developing countries in the matter of cyberthreat to constitute legal mechanism to tackle such unlawful acts.[4]

Internet is the one of most fast expanding sphere of technical framework infrastructure. So, Nowadays Information and communication technology systems are prevalent, and it accelerating the digitalisation trend. ICTs have significantly more impact on society than simply building basic information infrastructure. The availability and accessibilty of Information and Communication technologies system is a prerequisite for progress in the invention, availability, and use services of network based. Old Conventional written letters have replaced by electronic-mails, online site presence is now more crucial for firms than printed publicity materials, and Internet based communication (i.e. Online chatting or calling, sending mail) and wireless phone services are increasing faster than normal landline communications.

Now more individuals in developing nations could have easy access to the high speed Internet and related products and other services due to the smooth availability of long distance wireless communication technologies like Jio-Fiber Wifi and Airtel-Xtream wifi, as well as computer systems that are now available for cheap cost.

THE MAJOR CAUSES OF CYBERCRIMES

Cybercriminals usage the computer technology and internet to hack into user Desktops and laptops, smartphone data, social media profiles, company secrets, and national secrets, among other things. Hackers are criminals who engage in these unlawful acts via the internet. Despite the efforts of law enforcement authorities to combat the problem, it continues to spread, and many of people have become aggrieved of online fraud, hacking, identity theft and harmful dangerous software. Impenetrable security technology that uses an integrated system of software

[4] Prof. Dr. Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, 2012, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

andhardware to authenticate any information accessible over the Internet is one of the greatest ways to block these thieves and secure sensitive information.

Cyber criminals attack on the privileged or rich businesses, such as banks, casinos, and investment institutions, where large sums of money are exchanged on a daily basis, and steal critical information. After that becomes difficult to arrest these perpetrators as a result, number of cybercrimes increases all over the globe. Computer systems are sensitive, and regulations must be made to protect and secure them from cybercriminals. There are some following reasons why computers are vulnerable.

- **Easy to acesses**

  The main challenge with protecting and securing a computer systems from unauthorized access is that, due to some complex framework of technology, there are several methods for a violation to take place. Hackers can acquire login information, eyes retina scans, advanced audio-recorders, and other electronic-devices can easily deceive or mislead biometric (fingerprint systems) and infiltrate computer firewall also
- **Potential to store huge data in little space**

  The computer has potential to store and protect all data/information in a little space of storage, and it makes much easy for offenders to pilfer data from other storage of computers or laptops and take benefit from it.
- **Complexity**

  Computers run on operating systems such as (Window XP, Window 7 or Window 10), which are comprised of a large number of program coding. Because the mind of human being is not free from flaws, errors can occur at any time. Cybercriminal take benefits of these loopholes.
- **Negliance**

  Irresponsibility is one of the characteristics of human behaviour. As a matter of fact, there is a likelihood that while protecting the computer system, we will mess it up all the things that allows cyber-criminals access and control.
- **Evidence destruction**

Data in connection to the crime can be simply destroyed. As a result, destroying of evidence has become a very widespread concern and this evident concern has tried to disable the cybercrime investigation system.

CYBERCRIME DURING COVID-19 CHALLENGES

Inadequate knowledge or awareness, misuse or habituate to social media, and greater use of internet through which many people's trying to work online for earn some money during the (SARS) Covid19 outbreak are one of the causes for increasing cybercrime cases, according to the cyber experts. Facebook and Instagram have the most incidences of social media-related cybercrime.

Cybercrime is divided into two categories: corporate crime and individual crime. "The most of threats to a company's database affect corporate firms. They get hacked or have a large amount of traffic sent to the system. Cyber Criminals are targeting individuals largely as a result they become victim of cyber stalking, fraud online UPI payment and getting blackmailing in the times of social media. Cyber Criminals are growing more sophisticated, and they are taking advantage of the current trend to blackmail people. The bulk of folks have recently been deceived by bogus calls seeking vaccine booster doses. By submitting the OTP given by the hackers, citizens lose the money.

TYPES OF CYBER CRIME

Hacking - An attempt to manipulate a computer system or a private network within a computer is known as hacking or we can say misuse of computer devices, smartphone, or other digital devices for the purpose to commit illicit act.

Child Pornography and abuse - it means any content which portray sexual activity of child or exploitation which visualizes the sexual exploitation of child below the age of 18 years.

Piracy or Theft- When any person violates copyrights and illegal downloads music, movies, games, or software, they are committing a crime.

Cyber Stalking- Online harassment or abuse, which is a kind of "cyberbullying" and "in person stalking" can take the form of emails, text messages, social media posts, and other forms of communication, and is frequently systematic, purposeful, and continuous.

Cyber Terrorism- Computer-based attacks that try to disable important computer systems in order to attack, compel, or disrupt a government or a section of the public.

Identity theft-Identity theft occurs when someone impersonates you and usage your personal identity information to commit fraud or obtain other monetary benefits.

Computer Vandalism-is the act of cause harm or ruin to a computer system. Vandalizing a website, making malware that hamper or damages electronic documents or parts that disrupt the computer regular operation, or removing a drive to disable a computer system are all examples of cyber vandalism.

Malicious Software- Any software that is designed to damage or hack the user is classified as malicious software. They could be seeking to steal personal information, or could be acting maliciously

Phishing- It is a term that contains a wide range of internet schemes that 'phish' for individualspersonal and financial data (e.g., login id and passwords, Social Security Id Number, bank account detail, bank credit card numbers etc)

Fake News sharing in Social Media- sharing incorrect or misleading information, false sensitive news over the social media platform for disturbance of peace and tranquility in the society

Auction or Online retail fraud- it refers to fraudulent advertisement on auction websites. For eg:- Seller is selling product on website that do not exist or is selling the one good on the website to everyone who bid on the goods.

FEW METHODS OF CYBERCRIME INVESTIGATION

Tremendous technological advancements and improvements have occurred in the digital India for the uprising of Nation. With the development of technology, the number of offences involvingtechnology is too rising. Many cases have been filed under the Information Technology Act of 2000, such as Data and identity theft, hacking, illegal access to email account, child pornography, intellectual property theft, cyber terrorism attack, computer viruses, and other crimes have all been reported. Cybercrime has become a significant threat to business, national security, and the public at large[5]. Followings are the methods of Cybercrime Investigation

Inquiry

In this attempting to gather information related to crime, why this crime has done or who committed it, also to know how to proceed investigation.

Collecting Information

Evidence is occasionally gathered from the hacker's computers as well, through the examining of web cameras, wiretaps, and other means

Cyber Forensics

After completing the aforesaid steps i.e. the Inquiry and Collecting Information then Cyber Forensic tools are used to examining all the collected evidences, so after the examination of evidences should be preserve and collect carefully as it has to present before the court.

Approaches of Cyber Crime investigation-

- Track Internet Protocol (IP),
- Examination of Webserver Log,
- Inspection of Electronic mail Account,
- Attempting to retrieve distroyed evidences,
- Attempting to break the password,
- Try to extract concealed information that is not readily apparent.

TYPES OF INVESTIGATION

Internal investigations and civil investigations are the two most common forms of investigations. The standards get increasingly demanding with each type, and the penalties for noncompliance become more severe. Assume that the most stringent restrictions apply to all enquiries as a general rule.[6]

Internal Investigation

[5] M. Elavarasi and N. M. Elango,Analysis of Cybercrime Investigation Mechanism in India.

[6] DattatrayBhagwanDhainje, Cyber-crime investigations issues and challenges.

The most accessible inquiries you can undertake is an internal investigation. Internal investigation are more probably to be the least distressing form of professional investigation you will ever do. You work very closely with administration and the people whom you are investigating are unlikely to be aware of what you are doing until and unless you are completed. Need not to worry about courts and advocates to analyzing every single word you utter or write for the least mistake. We aren’t saying that internal investigations not governed by laws. Certainly, there are still some. Union and State privacy legislation apply to even the small corporations. Furthermore, each state has its own set of rules governing how corporations handle issues such as employment, implied privacy, and implied contracts. Most corporations have special policies and practices for to tackle such situations. In addition to a printed employee manual, a corporation's documented instructions covering issues that result to termination, how to use of company’s infrastructure includes various systems (such as computers, email services, and wireless network services) and so on are very likely to exist. At every level of the procedure, make sure you respect the law and company policy. If the conflict appears between the two, seek legal aid.

Civil Investigation

When intellectual property rights are in peril then civil instances are probably to be put forward to the institution, whenever an institutions network security has been compromised, also when corporation believes an employee or stranger is using the network without permission. For e.g.Abuse of resources, try to unauthorized access, malignant Communication etc. Any investigator investigating civil matter should be aware of the CPC, 1908. In this law degree is not required, only good understanding in civil law is beneficial.

CYBER CRIME INVESTIGATION CHALLENGES

As cybercrime is more sophisticated than other crimes, it should be investigated as soon as possible because evidence and facts in computer can be readily removed. There are some points which we can relate to Cybercrime Investigation Challenges[7]:-

Limited Access to data

As this cybercrime investigation is the part of a criminal investigation, may be law enforcement authorities refused access to computer data or have limited access to data. Rising technological growth and internet use serves as an obstacle for the Law Enforcement agency, it results in enormous amounts of data which creates complexity or difficulty to restrict and identify perpetrator of crime.

Location Problem

Nowadays, Cyber Offenders also uses E-Chiper to prevent revealing data or information from reaching of Law authorities, the advent of "crypto currencies, namely Ethereum. Bitcoin, ripple allows offenders to transaction in the illegal activities with a degree of secrecy Encryption, crypto currency, and different technology just like darknet (hidden web) or cloud

storage can cause loss of data, but it also become difficult and tough for law enforcement agencies to track down offenders, criminal organization, and technical evidences.

Ambiguity in Legal Framework

Because legal frameworks varies from country to country, investigating and penalising cybercrime beyond the territories is particularly challenging task. The significant distinction are in the types of activities which are criminalized and how investigations are carried out.

Whereas differences between countries frameworks make cooperation within other nations difficult, International cooperation is challenging in general due to the lack of a globally standard legal framework. This is mainly harmful when large-scale cyber-attacks take place beyond the territories.

Non-Cooperation Private Entities

Despite the significance of public-private partnerships. there is no specific legal regulatory structure governing how the private sector might cooperate with law enforcement.

[7] Nyman Gibson Miralis - Dennis Miralis https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f b7dc-cd91826f05d4.

CYBER INVESTIGATION LAWS IN INDIA

Certain special expertise and technical tools are required for performing cyber-crime. investigations: otherwise, the investigation would be useless. There some provisions of the t Criminal Procedure Code & Indian Evidence Act have been amended by the reason of Information Technology Act 2000. Further, the Indian legal system has enacted new legislation in response to need for Cybercrime investigations

Importance of Cyber Legislation in India

Cyber Legislation is crucial because it covers substantially all elements of transactions and activities on and with the Internet, the World Wide Web, and Cyber World At first sight, Cyber Legislations may seem to be a highly technical field with little relation to ordinary Cyberspace activities.Official data released by National Crime Record Bureau on 15 September 2021 stated that India50,035 cases of cybercrime recorded in the year 2020, increasing 11.8 % from the last year, also578 cases of "false news on social media reported As per NCRB Data, there were 4,047 instances of online banking fraud. 1,093 OTP frauds, 1,194 credit/debit card frands, and 2,160 cases of ATM fraud reported in year 2020.[8]

Who can investigate cyber offences?

The power to investigate related to cybercrimes under the section 78 of Information Technology Act, 2000, which expresses as "Notwith standing anything contained in the Criminal Procedure Code (CrPC), 1973, the Police officer not below the rank of Inspector shall investigate any offence under the Information Technology Act "[9] Even so, Information Technology Act is not sufficient to address the demand. As a result. Cr.PC, 1973 & IPC, 1860 were both legislations amended to embrace cybercrime in their scope This amendment empowers the Inspector to register and investigate cybercrime in the same way that he or she would committed any other crime.

[8] National Crime Records Bereau, https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE 9A_1.pdf

[9] InformationTechnologyAct,2000,Section78.

Procedure of Arrest and Seizure

Section 80 of the Information Technology Act, 2000 talks about power of police officer and other officers to enter, search etc., Section 80 (1) expresses that "Notwithstanding anything contained in the Criminal Procedure Code, 1973 "Any police officer not below the rank of the Inspector or any other officer of the Central Government or State Government authorized by the Central Government in this regard, may enter any public place, search and arrest without warrant any person, who is reasonably suspected of having committed or of committing or about to commit an offence under the Information Technology Act,2000

Following aforesaid, Section80 subsection (2) also expresses Any person who is arrested under section 80 subsection (1) by an officer other than a police officer then such officer shall without any unreasonable delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

Offence committed by Companies

If an illegal act is committed by the Company that is offence under the IT Act, “every person who, at the time the offence was committed, was in-charge of, and responsible to, the company for the conduct of the company's business as well as the company, will be guilty of the offence and will be prosecuted and punished in accordance with the Information Technology Act provisions”[10].

The Government of India has launched www.cybercrime.gov.in, an online cyber-crime reporting platform that is a citizen-centric attempt that allows complainant to lodge complaint against child porn or child sexual abuse or any sexually depicted content.

The (I4C)“Indian Cyber Crime Coordination Centre” has been setup by the Union Government to accost cybercrime events in India in an extensive and coordinated manner.

“National Cybercrime Threat Analytics Unit, National Cybercrime Forensic Laboratory, National Cybercrime Training Centre, National Cyber Research and Innovation Centre, Cybercrime Ecosystem Management ,Platform for Joint Cybercrime Investigation Team”.

Penalizing Cybercrime under the Legislative Laws

[10] Information Technology Act, 2000, Section85.

Some common cyber-crime instances that are subject to punishment under the Information Technology Act's relevant provisions are following:-

- *Online Hate Speech Group*

This is created to incite a different religious group to act or make derogatory and unpleasant remarks about a public figure, the country, or whatever else. This unlawful act can be prosecuted under Section 69 & 69A of the Information Technology Act, 2000 and Sections 153A, 153B & 505 of the Indian Penal Code, 1860

- *Hacking of Electronic Mail Account*

If an individual's electronic mail account is hacked, insulting or filthy emails are sent to the individual's address book. The following act can be prosecuted under Sections 43, 66, 66, 67, 67A and 67B of the Information Technology Act, 2000.

- *Webpage Deformation*

Sections 43, 66, 66F, 67 and 70 of the Information Technology Act, 2000, will be charged if the homepage of the website has been altered with a page with derogatory or obscene information.

- *Cyber Terrorism*

Terrorist uses virtual and physical storage to hide their unlawful business data and records. For this unlawful act UAPA Act and Sections 66 F and 69 of Information Technology Act, 2000

- *Phishing and email scams*

In this getting secret information fraudulently by imitating a trustworthy. It can be prosecuted under sections 66A and 66D of the Information Technology Act, 2000 and Section 420 of India Penal Code, 1860

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

https://www.ijalr.in/